TELECOM ParisTech

Une école de l'IMT

INSTITUT VEDECOM
DU VÉHICULE DÉCARBONÉ ET COMMUNICANT ET DE SA MOBILITÉ

12th ITS EUROPEAN CONGRESS
ITS BEYOND BORDERS
Strasbourg, France | 19-22 June 2017

Design and Verification of Secure Autonomous Vehicles

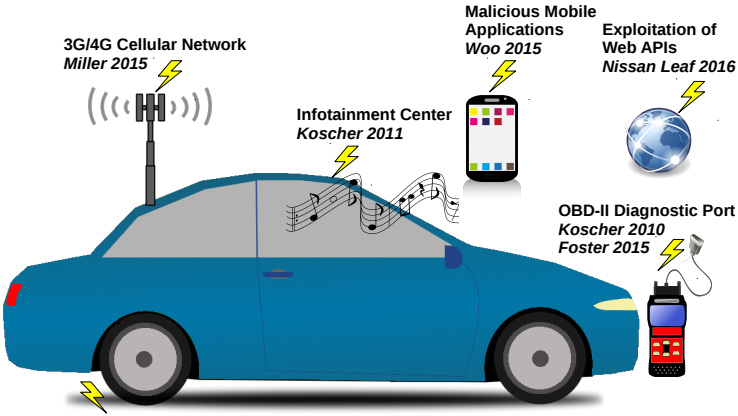
Letitia W. Li, Ludovic Apvrille, Annie Bracquemond
letitia.li@telecom-paristech.fr

Organised by: ERTICO ITS EUROPE

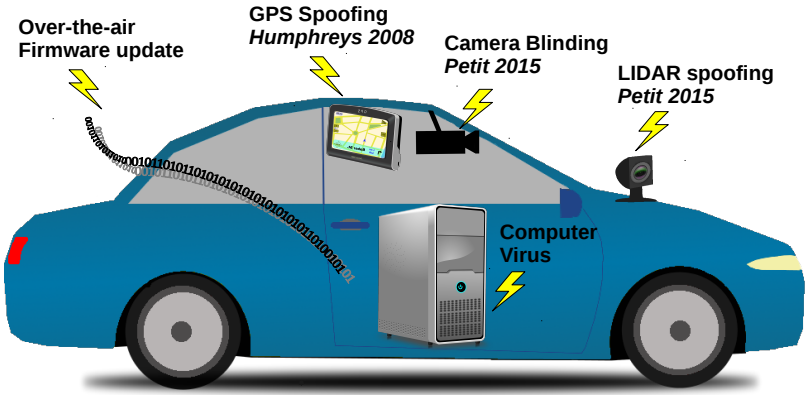
Hosted by: Strasbourg.eu

Supported by: AISACE, ITS FRANCE, STRASBOURG CONVENTION + EXHIBITION CENTRE, Cluster Pôle Véhicule du Futur, EURO

Attacks on Connected Vehicles



Attacks on Autonomous Vehicles



EVITA Project

- FP7 project ended in 2012
- E-safety Vehicle Intrusion Protected Applications
- Design of architecture for secure automotive on-board networks
- EVITA does not address side-channel attacks i.e. hardware is assumed to be tamper-resistant
- Several EVITA-compatible ECUs on the market (STM, Bosch, etc.)

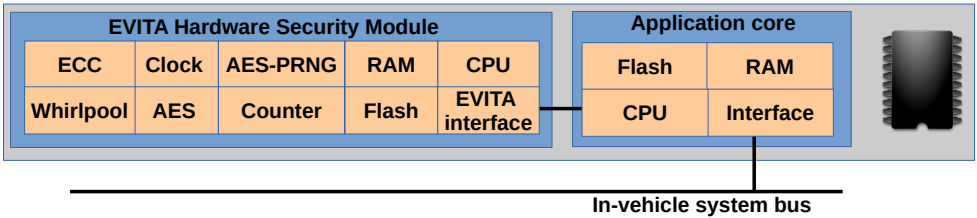
Security Requirements

- Authenticity of vehicle software and data
- Authenticity of vehicle communication
- Confidentiality of vehicle communication
- Integrity of vehicule communication
- ...

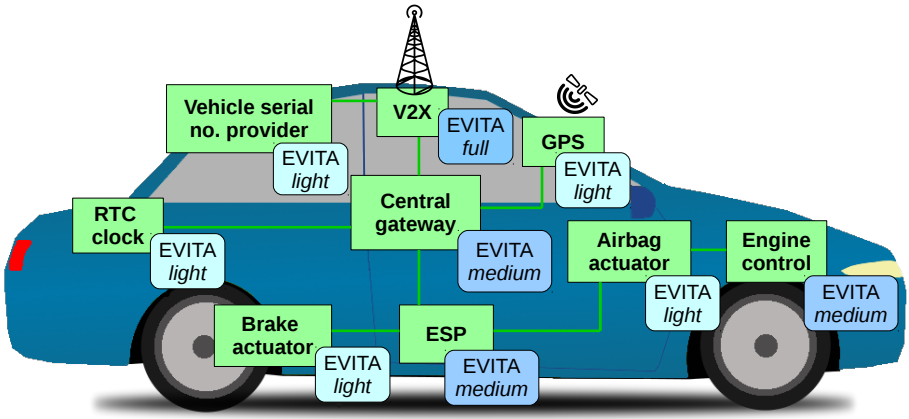
EVITA Results

- Security Protocols
  - Protocols are CAN compatible
  - Formally verified with SysML-Sec
- APIs
  - Integration in Autosar
- Specification of Hardware Security Modules

Hardware Security Modules



EVITA Architecture



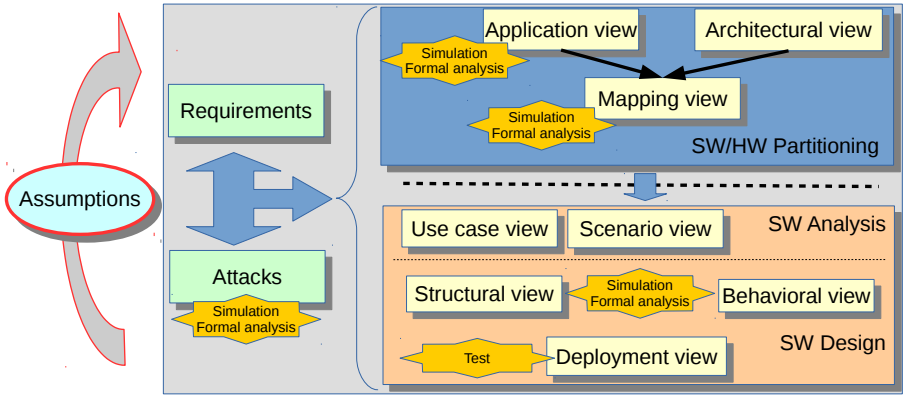
How to Design a Secure Automotive System?

"Those who fail to plan, plan to fail."

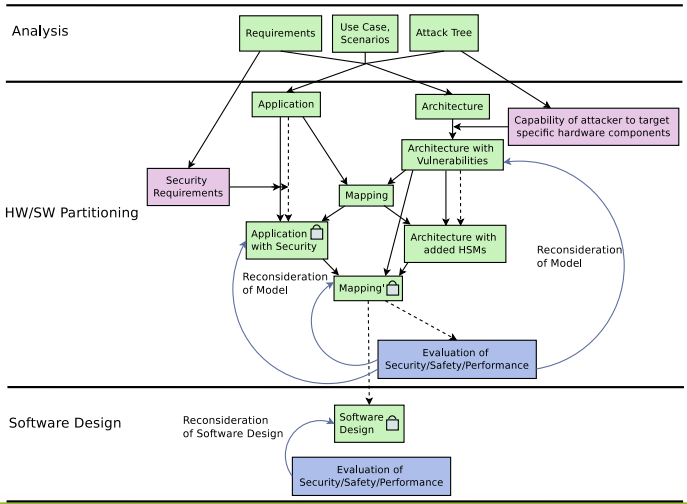
Benjamin Franklin

- Use of a model-driven approach (**SysML-Sec**)
- Support of safety, performance and **security** (formal) verification

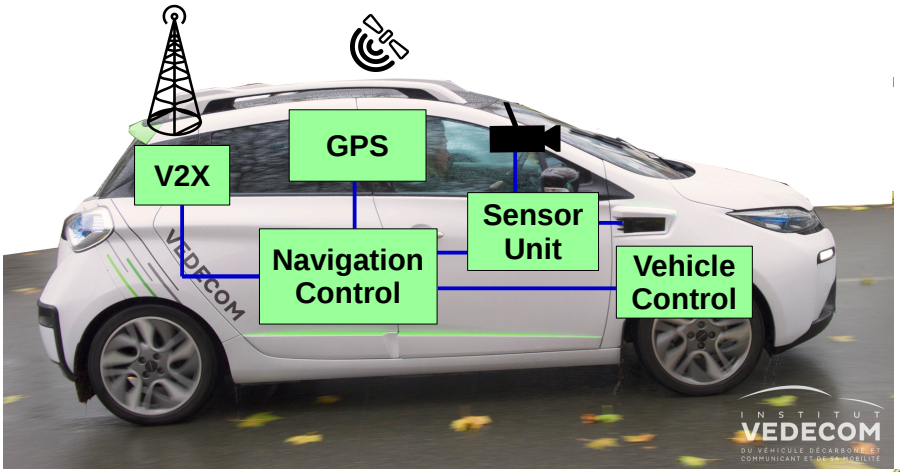
SysML-Sec Methodology



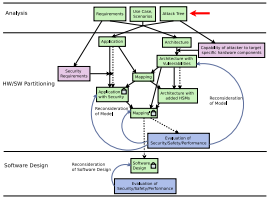
Methodology in detail

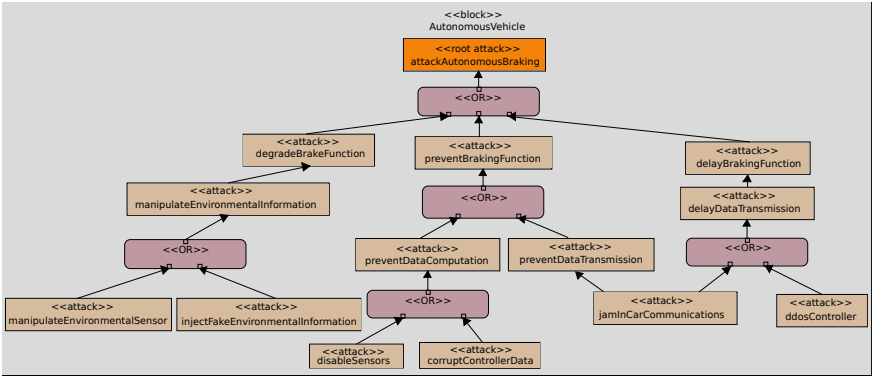


Autonomous Vehicle under Design

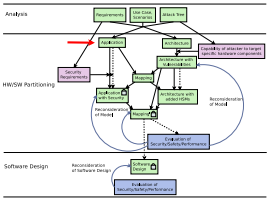


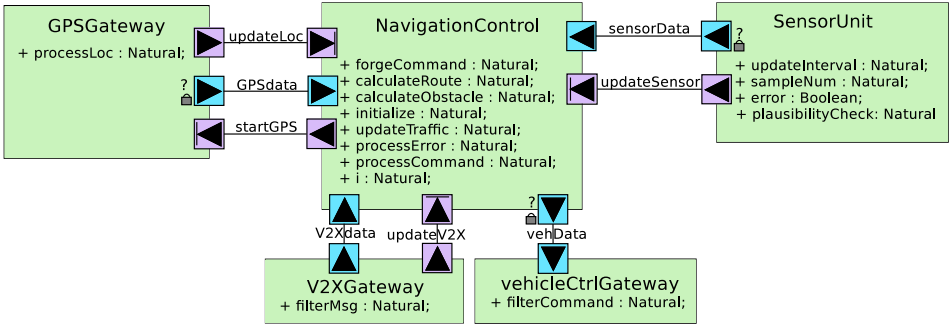
Attack Tree


Analysis
Requirements
Use Case Sub-cases
Attack Tree
Application
Architecture
Capabilities of attacker to target specific hardware components
Security Requirements
Requirements
Architecture with Hardware (HSM)
HW/SW Partitioning
Application with Security
Architecture with added HSMs
Reconsideration of Hazard
Reconsideration of Hazard
Hazards
Evaluation of Security Functions Performance
Software Design
Reconsideration of Software Design
Software Design
Evaluation of Security Functions Performance

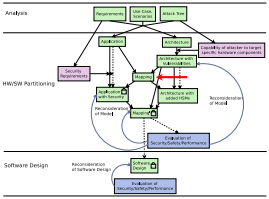

<<block>>
AutonomousVehicle
<<root attack>>
attackAutonomousBraking
<<OR>>
<<attack>>
degradeBrakeFunction
<<attack>>
preventBrakingFunction
<<attack>>
delayBrakingFunction
<<attack>>
manipulateEnvironmentalInformation
<<OR>>
<<attack>>
delayDataTransmission
<<OR>>
<<attack>>
preventDataComputation
<<attack>>
preventDataTransmission
<<OR>>
<<attack>>
manipulateEnvironmentalSensor
<<attack>>
injectFakeEnvironmentalInformation
<<OR>>
<<attack>>
jamInCarCommunications
<<attack>>
ddosController
<<attack>>
disableSensors
<<attack>>
corruptControllerData

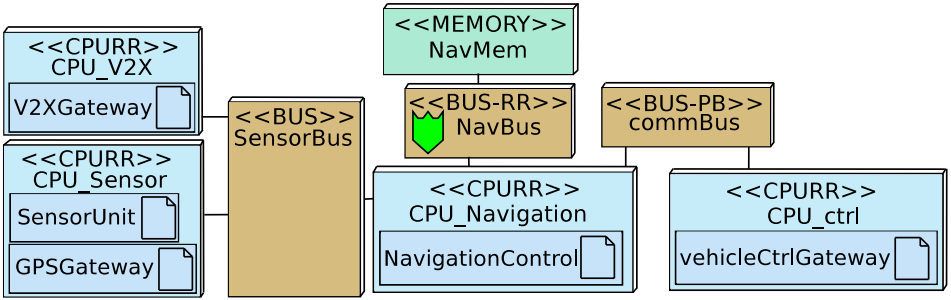
Application View



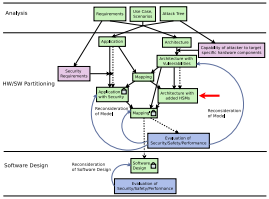


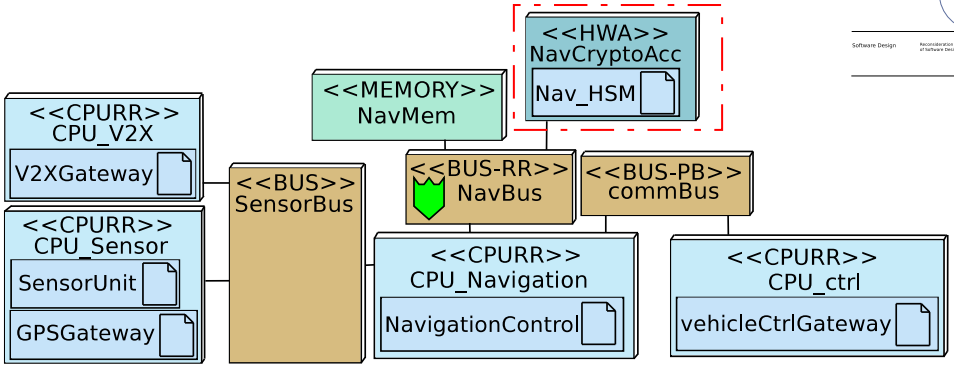
Architecture/Mapping View



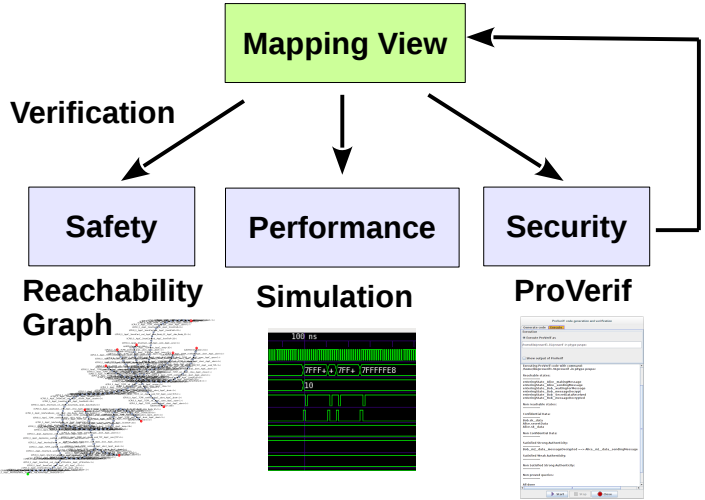


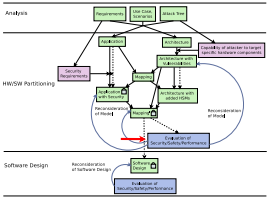
Hardware Security Modules



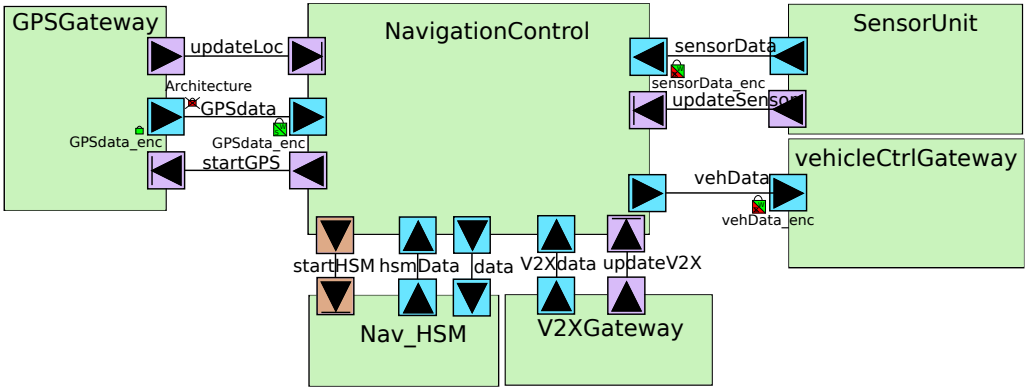


Model Verification





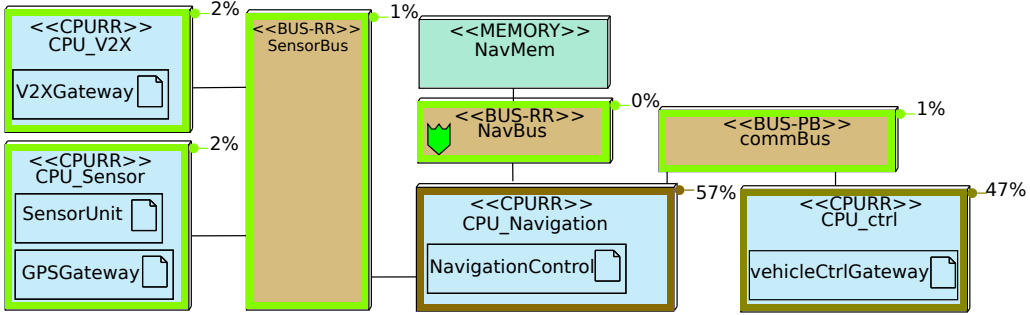
Security Verification Results



Impact of Security on Performance and Safety

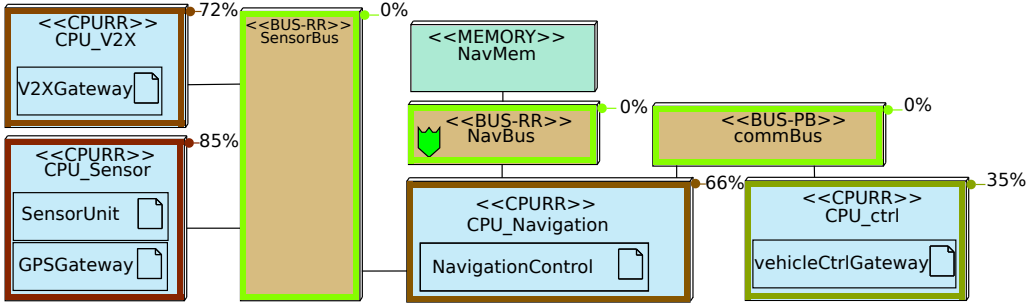
- Encryption/Decryption occupy execution cycles
- Communications increase due to key exchange, increased message size

Model Simulation



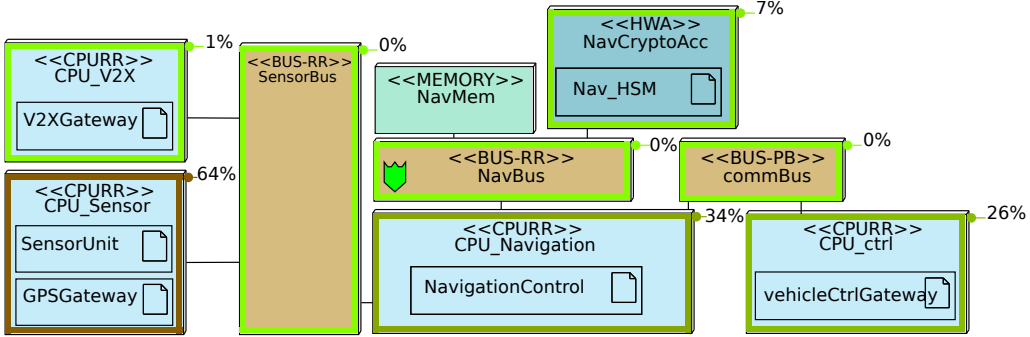
14000 cycles

Secured Model



17000 cycles

Secured with HSM



16000 cycles

Test of Security Countermeasures

Conclusion and Future Work

Contributions

- New security considerations for autonomous vehicles
- Increased connectivity introduces vulnerabilities
- Model-Driven approach towards modeling and verification of (automotive) embedded systems

Future Development

- Iterations betwen requirements, attacks and partitioning solutions
- Modeling the relationship between safety and security
- Better relations between partitioning and subsequent modeling stages

Thank You!

References

TTool: ttool.telecom-paristech.fr

SysML-Sec:
http://sysml-sec.telecom-paristech.fr/

Personal website:
http://perso.telecom-paristech.fr/~apvrille